

AD-A114 399

ARMY SCIENCE BOARD WASHINGTON DC
THE CHALLENGE OF TERRORISM TO THE MILITARY. (U)
MAR 82 R H KUPPERMAN

F/6 5/11

UNCLASSIFIED

NL

1 of 1
62-882



END
DATE
FILMED
6-82
DTIC

12



DEPARTMENT OF THE ARMY
ASSISTANT SECRETARY OF THE ARMY
RESEARCH, DEVELOPMENT, AND ACQUISITION
WASHINGTON, D. C. 20310

A ARMY
S SCIENCE
B BOARD

MAIL

THE CHALLENGE OF TERRORISM
TO THE MILITARY

MARCH, 1982

DTIC
ELECTE
MAY 13 1982
H

DTIC FILE COPY

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

82 05 12 075

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A114319	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Army Science Board Report The Challenge of Terrorism to the Military		5. TYPE OF REPORT & PERIOD COVERED Final
7. AUTHOR(s) Kupperman, Robert H.		6. PERFORMING ORG. REPORT NUMBER
9. PERFORMING ORGANIZATION NAME AND ADDRESS Army Science Board, Office Assistant Secretary of the Army (Research, Development & Acquisition) Washington, DC 20310		8. CONTRACT OR GRANT NUMBER(s)
11. CONTROLLING OFFICE NAME AND ADDRESS Army Science Board Office Assistant Secretary of the Army (RDA) Washington, DC 20310		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE March 1982
		13. NUMBER OF PAGES 16
		15. SECURITY CLASS. (of this report)
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This report examines the challenge of terrorism to the military. Specific items addressed are past and future terrorism concerns, including terrorist incidents, problems of hostages, terrorist arsenals, plausibility of mass destruction terrorism, conventional weapons, unconventional weapons, bacteriological warfare as a terrorist weapon, chemical warfare agents and technological challenges ahead.		

DD FORM 1473

JAN 73

EDITION OF 1 NOV 63 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

THE CHALLENGE OF TERRORISM TO THE MILITARY

by

ROBERT H. KUPPERMAN



Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A	

CONTENTS

Introduction.....	1
Background of the Battleground.....	3
Terrorist Incidents.....	3
Problems of Hostages.....	4
The Terrorist Arsenal.....	6
The Plausibility of Mass Destruction Terrorism.....	7
Conventional Weapons.....	9
Unconventional Weapons.....	10
Bacteriological Warfare as a Terrorist Weapon.....	10
Chemical Warfare Agents.....	12
Technological Challenges Ahead.....	13

INTRODUCTION

No terrorist organization rivals the smallest standing army. Not even the larger and more sophisticated Palestinian groups, such as the Popular Front for the Liberation of Palestine (PFLP), is a military match for the smallest fighting unit within the United States Army. At the same time, civil authorities may be unable to cope with terrorism on a full time basis, particularly when terrorist acts are directed against the military. Self-defense, or an even broader role, might be appropriate for the army.

Before proceeding further, it is important to understand that terrorists cannot operate in direct combat successfully during wartime. Once an army is on the move and prepared to accept casualties, the terrorist is of little or no importance. During World War II, the Korean conflict, and the Vietnam debacle, the United States Army had been prey to special operations of the enemy, including sabotage, guerrilla tactics, and psychological warfare.

The military's problem with terrorism occurs during peacetime or during the precarious transition between highly unstable political conditions in a strategically important area and the outbreak of armed conflict. Low-level fighting, including terrorist assault and other such violence, can start an unraveling effect leading to substantial military confrontation.

The 1980's promises to be a decade of terrorism and unconventional warfare. The strategic balance between the United States and the Soviet Union is not favorable to the West. The United States and its allies can no longer dictate the course of political and military events. NATO has eroded politically and militarily, and a slow "Finlandization" of Europe appears possible. Further, the mid-50's image of bipolar confrontation has been transformed to an ambiguous multi-actor game in which the United States plays a decreasingly important role. Terrorism fits in with today's geopolitical realities, not within the bipolar framework of the past, particularly, bearing upon Alliance relationships. For example, were terrorists to attack a nuclear weapons storage facility in Europe, the affected European government might demand the removal of all nuclear weapons. The United States would be obliged to do so, even at the risk of dismantling NATO.

Although the United States and NATO have invested substantially in physical security as well as command, control, and communications at an operational level, Alliance and national authorities are relatively unprepared to handle terrorist crises at a political level. Complicating matters is America's disbelief in the Delta force as a result of the failure of the Iranian rescue mission. A claim that the Delta force or other U.S. response teams could successfully cope with a hostage siege at a sensitive installation would appear incredible. Thus, the United States faces both the operational realities of coping with a terrorist event and the political reality of past failure.

In addition to the peculiar problems of protecting nuclear weapons, chemical weapons, and portable surface-to-air rockets, the U.S. military may experience terrorist incidents disrupting the industrial mobilization base and industrial infrastructure. Additional technical problems, including the detection and identification of chemical and biological weapons and the cleanup following such a terrorist attack, need to be resolved expeditiously.

The military of many Western countries may be faced with a variety of problems resulting from terrorist attacks. Until recently, terrorist tactics were largely limited to assassinations, bombings, kidnappings, and hostage taking. However, more technologically sophisticated assaults, including attacks on electrical power systems, computer networks, maritime facilities, and refineries, may be anticipated.

While Americans and American interests abroad have regularly been victimized by South American, German, and Palestinian groups, the American public has viewed terrorism as a distant, foreign problem—not a serious domestic concern, other than that the phenomenon has been loosely lumped with the more general and pervasive problem of violent crime. The Iranian siege changed matters substantially. The United States, a super power tarnished by its defeat in Vietnam, was again demeaned, held at bay for more than a year. Diplomacy, economic sanctions, international condemnation, and the prestige of America failed to move the Iranians. The final embassassment for America—and eventually the loss of the Presidency for Jimmy Carter—took place in the Iranian desert. All that was left was a "rug bazaar", negotiating the price to release the hostages. America failed diplomatically and militarily to deal in proportionate term with terrorists; a national disaster was the result. The military appeared impotent, capable only of inflicting nuclear carnage or acquiescence.

The Iranian episode is not an isolated matter. Viewed as a form of warfare, as unimpressive in firepower terms as it was, such incidents and other highly leveraged terrorist assaults may become the norm of conflict in the 80's. Terrorist attacks are not clean. Often convert at the onset and difficult to predict, terrorism has become a new breed of surrogate conflict, making large-scale conventional and nuclear warfare the likely consequence of failing to cope at a molecular level of violence.

Few generals and admirals understand terrorism well. They count ships, aircraft, tanks, large artillery pieces, and troops. They search for the forward edges of the battle area (or forward lines of troops), and they expect comparable conduct of their enemies. Laws of war, traditional tactics, and standard rules of engagement are ingrained in military thinking. Terrorists do not adhere to the traditions of West Point or Annapolis; rather they are dedicated, sophisticated, and cunning, employing ghetto tactics in an elitist setting.

Counterterrorism and special operations will be a part of tomorrow's military chess game. NATO's electronic battlefield may prove too expensive a playground for all concerned. The perceived thresholds between the terrorist event, regional destabilization, limited conflict, and the opening of the nuclear Pandora's box will continue to erode dramatically.

Because terrorism is the de facto partner of the media, it has become a dynamic theatrical endeavor whose producers fear complacency. Terrorist tactics must change if they are to compete with governments' efforts to combat terrorism and if they are to ensure a shocked, frightened public. Adaptation is therefore inevitable if government impotence is to be guaranteed. The spectrum of terrorist attacks will enlarge to include the downing of commercial aircraft, attacks on nuclear weapons storage facilities, and the possible use of chemical, biological, and radiological agents. The United States military cannot escape; there is no retreat to World War II. Not only must serious contingency planning and innovation become important ingredients of military thinking, it is important to redirect emphasis from more conventional R&D efforts to the more elusive problems of counterterrorism.

BACKGROUND OF THE BATTLEGROUND

Since 1977, the public concern over terrorism has grown. Recent declarations by President Reagan and Secretary of State Alexander M. Haig, Jr., indicate that the government shares the sentiment that it is a serious problem. The hostage crisis in Iran, coupled with recent attempts to assassinate Pope John Paul II, General Kroesen, and others, have alerted the American public to the perils that the specter terrorism can hold for a democratic society.

In the past decade, terrorists have elevated the arts of assassination, hijacking and kidnapping, arson and bombing, and extortion. As a result of such efforts, terrorists have occasionally succeeded in causing a paralysis among Western nations. At times, the West has capitulated to terrorist terms, examples being the releasing of Iranian assets to settle the Teheran Embassy-hostage crisis, and the freeing of Abu Daoud in 1977 by France, notwithstanding his involvement in the 1972 Munich Olympic massacre of Israeli athletes. The lack of either a unified response to terrorism among the allies or a plan of positive counterterrorism has left the West vulnerable to continued terrorist attacks and pressures.

Terrorist Incidents

Terrorist organizations have engaged in a wide number of activities, many showing an unusual ability for adaptation. The PFLP and its related factions have hijacked airliners on numerous occasions, the most spectacular incident involved the destruction of several jets in Jordan in 1970. Palestinian operatives kidnapped OPEC oil ministers in 1975 and assisted the supporters of Ayatollah Khomeini in Iran during the hostage crisis in 1979. Kidnapping and murder have been a part of the Baadner-Meinhof and Red Brigade actions against Hans-Martin Schleyer and Aldo Moro in West Germany and Italy, respectively. The Lod Airport massacre in Israel in 1972 featured members of the Japanese United Red Army while targeted assassination of selected individuals has characterized IRA actions, as evidenced in the bombing death of Lord Mountbatten in 1979.

In the last year, Red Army Faction (RAF), Fatah, Dev Sol, ETA, PLA, "criminals", and others have made 17 classified attacks against the US military in addition to the publicly acknowledge events noted in the table on page 4. [†]

TERRORIST ATTACKS AGAINST U.S. MILITARY

<u>DATE</u>	<u>TYPE EVENT</u>	<u>LOCATION</u>	<u>GROUP</u>
16 Sep 81	Bombings	Frankfurt, Germany	Unknown
15 Sep 81	Assassination Attempt	Heidelberg, Germany	RAF
1 Sep 81	Firebomb-Car	West Germany	Unknown
31 Aug 81	Bomb-Car	West Germany	RAF
18 Aug 81	Bombings	West Berlin	Unknown
8 Aug 81	Bombing-Car	Turkey	Unknown
17 Jun 81	Bombing	West Germany	Unknown
24 May 81	Bombing	Greece	ELA
16 Apr 81	Bombings	West Germany	RAF
6 Apr 81	Assassination	Turkey	MLAPU
3 Apr 81	Bombing	Greece	Unknown
30 Mar 81	Bombing	West Germany	RAF
29 Mar 81	Bombing	West Germany	RAF'
20 Mar 81	Bombing	Costa Rica	Paribundo Marti
17 Mar 81	Bombing	Costa Rica	Paribundo Marti
2 Feb 81	Bombing	West Germany	Unknown
22 Jan 81	Assassination	Turkey	MLAPU
29 Dec 80	Bombing	Greece	Unknown
27 Nov 80	Bombing	Turkey	Turk Rev Youth Fed.
25 Nov 80	Bombing	Turkey	Dev Sol
15 Nov 80	Assassination	Turkey	MLA
2 Oct 80	Bombing	Turkey	Dev Sol

In the United States, the anti-capitalist New World Liberation Front, consisting of many former Weather Underground members, has frequently sabotaged energy facilities in California. The FALN, a Puerto Rican Nationalist group with significant support from Cuba, has fostered violence throughout Puerto Rico and parts of the United States, including New York City. Foreign nations have also acted in the United States through surrogates operating as assassins, the most notable being the Qadaffi government in Libya and the Khomeini regime in Iran.

Problems of Hostages

Hostage taking is an increasing problem in terrorist situations. The Iran Crisis and, more recently, the hijacked Pakistani airliner demonstrate a trend toward yielding to terrorists' demands. Only Israel has remained steadfast in refusing to negotiate with hostage takers. The taking of hostages is a volatile act that can catch both the terrorist and the intended target off guard. Once the hostages are secured, the terrorist is confronted with the problem of guarding and maintaining captivities. For the object of the terrorists' concerns, the hostages are emotional symbols and their safe release can become a preoccupation over and above anything else.

¹ Source: Army Times, September 28, 1981

Past hostage incidents have been among the most spectacular acts of terrorism, allowing for full media attention. The crisis in Teheran was carefully orchestrated by the militants who seized the U.S. Embassy with the encouragement and support of Khomeini's followers. During the initial months of crisis, and on special occasions, mobs converged on the embassy compound, allegedly demonstrating their opposition to the United States, thereby directing attention away from the plight of the hostages. Even more, the hostages were accused of being CIA spies and were threatened with trials and execution. The seizure of the embassy and U.S. hostages was a media event from the first day to the last; this was obvious to the militants, who played before the cameras and the members of the media.

The hijacking of the Air France jet to Entebbe in June-July 1976 was also a media event of major proportions. The PFLP and Baader-Meinhof agents involved in the plane's seizure had hundreds of hostages from many different countries. Everything about the crisis, from the capture of the plane to the listing of demands, to separation of passengers into categories, to the release of some hostages, all contributed to the drama. As in Iran, the host country (in this case Uganda) was intricately involved in the incident, supporting the terrorists and giving assistance.

The taking of hostages has proven to be an effective terrorist weapon. Unlike planned raids against unknown persons or acts of indiscriminate sabotage, hostage taking allows the terrorist to know the captive and the captive to become known to the world. The general response of the West to the practice has been capitulation; France and West Germany being prime examples.

The relative success of hostage taking should cause a rethinking of response to such acts. As the crisis in Teheran showed, the fifty-four Americans become so well known that any action taken that could have jeopardized their lives would have met severe criticism. The militants in Iran knew this and acted accordingly, allowing for movie taking at the holidays and so on. The result was that U.S. television made the hostages a part of everyone's life. The public's reaction against the aborted rescue mission in April 1980 is evidence of the militants' propaganda success.

Hostage taking in a nuclear plant or a similar sensitive site raises the issue of whether or not the captives' lives should be sacrificed for the greater good. Time invariably works to the terrorist's advantage, since it allows for consolidation and strategy planning. Frequently, a delay in responding to initial terrorist demands can lead to even greater demands being issued. The kind of widespread damage possible at a nuclear facility (witness Three Mile Island) suggests a publicly announced policy for such cases to include plans for an attack on the terrorists, even if that could lead to the death of the hostages. It is less costly for society to lose fifty or one hundred hostages if tens of thousands of potential victims can be saved.

The precedent for successfully attacking terrorists and rescuing hostages is the Israeli raid at Entebbe on July 4, 1976. The skillful planning and execution by the Israelis surprised everyone involved, especially the Ugandan Army. Terrorists are usually expecting acquiescence to their actions in a hostage situation. The hazard of continued acquiescence, especially in nuclear situations, is profound.

The Symbionese Liberation Army (SLA) actions in the early 1970's, especially the Patty Hearst affair, bothered the finer sensibilities of Americans, but did not really drive home the need for counterterrorism programs. America's friends abroad have tried to alert this nation to the terrorist threat,

but have often met with disbelief and indifference: "In the past, one occasionally...detected irritation on the part of some European officials at what they perceived as a cavalier attitude of the American government toward the problem of terrorism, which U.S. officials tended to see as a European disease, rather than as a problem affecting all modern, democratic, and comparatively affluent industrialized societies. In the European view, we in America simply did not take the problem seriously enough. If there was an underlying someday-you'll-get-yours resentment, the seizure of the American Embassy in Teheran probably wiped it out. Prior to that event there was a feeling abroad that neither the American government nor the American people fully appreciated the extent to which a single terrorist incident could mesmerize a nation and thoroughly divert its government. The Israelis during the Entebbe incident, the Dutch after the South Moluccans seized 100 school children, the Germans after the kidnapping of Hans Martin Schleyer, and the Lufthansa hijacking, or the Italians after kidnapping of their former premier Aldo Moro, could have told us."²

The Terrorist Arsenal

Compared with the tools of modern warfare, the arsenal of terrorists is usually primitive. Thus far, terrorists have rarely used more exotic weapons than pistols, submachine guns, grenade launchers, and crude bombs. Yet terrorists have achieved considerable tactical success.

An increased degree of sophistication of the terrorist arsenal could be marked by the use of more advanced weaponry and by the use of the present simpler weapons to attack more technologically sophisticated targets. Man-portable antitank and surface-to-air rocketry, chemical and biological agents, and nuclear weapons would fall into the first category. Use of explosives to knock out a main transformer of the electric power grid, sabotage against crude oil or natural gas pipelines, and destruction of critical computer installations fall into the second category. Terrorism could feasibly take on new and more harmful forms, possibly including mass-destruction weapons. The existence of alternative weapons and the consequent opportunities for implicit or explicit extortion pose a severe threat.

As is clearly the case for the Germans, Palestinians, Basques, and some South Americans, terrorists have access to machine shops and university-level laboratory facilities. It is assumed that they might employ a handful of Ph.D.-level scientists and engineers. Illustrating the reasonableness of this last assumption is the fact that several tens of thousands of Arab students have received graduate-level technical training in the United States and Western Europe; at least a few may actively support the more extreme Palestinian groups.

Biological and chemical agents, though readily attainable, have remained largely unused in conventional wars, insurgencies, or other violence. Documentation of incidents of the use of biological and chemical agents since World War I exists. The recent reports concerning "yellow rain" in Kampuchea, Laos, and Afghanistan and the outbreak of anthrax in Sverdlovsk indicate Soviet, client state, or supported terrorist threats. The Egyptian Army was reported to have used toxic agents against the Yemenites in 1967.

²Jenkins, Brian Michael, "Terrorism in the United States", TVI Journal, Vol. I, No. 4, March 1980

There are also reports that the Baader-Meinhof group recently threatened to use mustard gas against West German cities. In many respects, chemical and biological agents represent the terrorist's easiest avenue into the mass-destruction arena. In contrast to the concern over nuclear materials, the control and safeguard of chemical and biological agents have not been given adequate consideration. This is due, in part, to the ready availability of toxic chemicals, formulae for agents, and disease cultures. Indeed, it is far easier to culture anthrax than it is to steal or fabricate a nuclear device; a biological attack is potentially more lethal than a nuclear explosion. A small nuclear device could kill a hundred thousand people if detonated in a dense population center. By contrast, an aerosol anthrax attack could rival the effects of a thermonuclear device.

Few terrorist attacks have demonstrated technical sophistication. Nevertheless, isolated incidents of assaults involving the use of highly toxic agents and at least fifty threats to employ nuclear weapons in the United States have occurred. Iodine-131, a radioisotope, has been sprinkled over a train in Europe. The so-called alphabet bomber in Los Angeles developed sophisticated explosives and, when arrested, was apparently attempting to synthesize a nerve agent. In January 1972, two college youths were charged with conspiracy to commit murder in a plot to poison Chicago's water supply with "typhoid and other deadly bacteria." West German authorities, a year later, received similar threats of the introduction of anthrax into the country's water supply.

These threats did not involve complex technology, but they underscore the fact that there are people willing to threaten society and, possibly, willing to kill thousands of people. These people should not be confused with rational terrorist groups who have shown no predisposition to engage in acts of extreme violence. However, not all terrorists calculate rationally. Technology is here and governments must attempt to minimize terrorist ability to use it. Although mass destruction may not be likely, other far less violent acts of national disruption are.

Advanced societies are extremely vulnerable. The electric power grid, water supply systems, computer systems, computer networks, natural gas and crude oil pipelines, and airline transportation systems are examples of highly sensitive targets. The loss of critical components of any one of these systems could prove catastrophic. Few seriously conceived countermeasures have been taken to minimize these vulnerabilities. Indeed, the terrorist's task of disrupting vital networks has become easier with the advent of small, highly portable precision-guided antitank and antiaircraft rockets which terrorists have obtained, virtually all of them Soviet-made. The attempted assassination of General Fritz Kroesen involved an RPG-7 rocket launcher.

The Plausibility of Mass-Destruction Terrorism

Speculations about terrorist use of mass-destruction weaponry have been characterized as wild and sensational. It is often argued that terrorist use of such weaponry is unlikely for several compelling reasons. First, safeguards against terrorist access to suitable nuclear materials should

prevent such incidents. Second, biological and chemical agents have long been available, but have been used rarely and then ineptly. Third and perhaps most importantly, the use of mass-destruction weaponry would be counterproductive to terrorists—alienating followers and potential supporters and provoking much more repressive countermeasures. Although these arguments hold for the past and perhaps for the immediate future, governments and publics alike should anticipate developments that would make these arguments less persuasive.

The current trend toward proliferation of fissile materials and nuclear weaponry has underscored the erosion of superpower dominance and has been accompanied by increasing Third World militancy. Agreements precluding the use of nuclear, chemicals, or biological weapons may be beyond the ability of impoverished nations to enforce; such agreements are not binding upon terrorist groups.

As the ability to create nuclear weapons spreads, more countries may seek deterrents. Finding the nuclear alternative impractical, some may seek more rapidly accessible but equally potent forms of destructive capability, such as biological weapons. Although the penalties for using these mass-destruction agents may be too high for industrialized and developing nations, extremely poor national and certain subnational groups may be less cautious. The possession of mass-destruction weapons might be viewed as a quick route to political recognition by groups or countries with heretofore marginal political power. It is also possible that a mass-destruction capability will come to be perceived as a lever in the struggle for redistribution of economic and political power. The extortion potential will always be high where the capacity for massive violence is present; hostage situations of the future may involve entire populations.

Thus the arguments against the plausibility of national or terrorist use of mass-destruction agents may not be as compelling, for the longer term, as they now appear. First, even the best protected nuclear installations are subject to attack. The United States possesses no monopoly of nuclear technology and may not be able to assure the use of safeguards and physical security throughout the world. National accountability for fuels of nuclear plants in Third World countries may not be any better than their accountability in other matters. France and Italy were responsible for helping Iraq develop the reactor destroyed by Israel in June 1981. Moreover, corruption could create flourishing black markets in such materials if government or subnational groups are determined to acquire them for weapons production.

Security in nuclear energy plants outside the United States or Britain are not always of a high degree, and there is a possibility of terrorists holding a plant in a hostage-barricade situation, threatening leakage or other sabotage unless demands are met. For many, this scenario is more plausible than that of terrorists obtaining fissile material and constructing a nuclear bomb. There have reportedly been several instances of college students attempting to design a fission bomb—but most of these designs are of dubious validity; some are not.

Second, nations have demonstrated their willingness to use biological or chemical agents. Numerous examples of the use of chemical and biological agents since World War I exist. Such agents may grow increasingly attractive as a sort of "poor man's deterrent", as they are inexpensive, readily attainable, and effective.

The third argument against terrorist use of mass-destruction weaponry, based upon the alienating effects on supporters and worldwide opinion, may be the most cogent. But recent terrorist trends may make even this argument less convincing. Terrorist groups have not been deterred from widespread killing, as shown by the Rome and Lod airport and Bologna railway station massacres. Mass-destruction weaponry may prove highly appealing to nihilistic groups bent on causing shockingly destructive incidents. Apolitical, criminal groups might also be attracted to lucrative opportunities for mass-destruction extortion.

Radical factions of many terrorist movements such as the Palestinian "Rejection Front" may not fear the alienation of world opinion and may be attracted to mass destruction in the pursuit of their disruptive goals. Repressive governmental countermeasures that may discredit a democratic government are certainly one terrorist goal, just as insurgents seek to attract supporters by exposing the government as weak, then as ineffective, then as a police state.

Successful extortion and the undermining of national decision-making processes do not require actual use of such weapons by terrorists. The possession of mass-destruction agents, whether accompanied by the threat of use or not, by a terrorist group would focus widespread publicity on their cause and could provide significant political leverage.

No amount of theorizing can decide whether incidents of mass destruction will or will not occur. But one tenet is obvious—even if mass-destruction terrorism were highly improbable, potential consequences could not be ignored. It is necessary to try to understand the physical as well as the more complex socioeconomic effects of heightened acts of terrorism. The easier task is the assessment of physical effects, discussed next.

Conventional Weapons

It is difficult to assess and predict the plans of various terrorist groups. It is similarly difficult to know which weapons they might use. But because of availability and previous use, there are certain weapons that we must expect to find in terrorist hands.

The most readily available weapon to a terrorist organization is the crude, homemade explosive that can be fabricated from seemingly innocuous materials found on the open market. Next in availability is the automatic weapon. Typical examples are submachine guns and machine pistols made in the Soviet Union, Czechoslovakia, and Poland. Such weapons have been used extensively in terrorist operations. By contrast, heavy machine guns, such as the U.S. 50 caliber, are difficult to conceal and to move covertly. Light antitank

rocket launchers, principally the Soviet-made RPG-7 and the U.S. LAW, are known to be in the hands of terrorist groups. For example, the RPG-7 was used in the January 1975 attack on El Al Airlines at the Orly Airport, Paris. The U.S. LAW and other antitank weapons, such as the French Strim F-1, have been issued in quantity to the military forces of various nations. They are portable and easy to conceal. Surface-to-air missiles, while the least readily available of the weapons discussed, are known to be in the possession of Palestinian groups. Defenses (e.g., Kevlar body armor) and armaments for counterterrorist forces (civil or military) are inherent in Army equipment, particularly test items in The High Technology Test Bed (9th Infantry Division, Fort Lewis).

Unconventional Weapons

The development of radiological weapons (excluding construction of a nuclear explosive), the synthesis of nerve agents, and the culturing of small amounts of suitable biologicals are straightforward matters that are discussed today in the open literature. Moreover, dangerous agents such as cobalt-60, the insecticide TEPP, and specimens of anthrax, Venezuelan equine encephalitis, smallpox and other diseases are generally available. Although growing virulent biologicals is a hazardous activity for the amateur and making large quantities takes considerable skill and judgment, many thousands of people are sufficiently trained to perform such tasks.

It is easy to theorize about nuclear explosives, virulent toxins, and live pathogens, but there is a wide gulf between the theoretical and the practical. Though theoretical construction of nuclear explosives has become an armchair pastime, the fabrication of a reliable nuclear explosive is a difficult and dangerous task that would not be undertaken lightly by a terrorist organization wishing to preserve its meager technical assets, especially its scientific personnel. Similarly, though theoretical estimates of casualties from chemical, biological, and radiological attacks are easily made, the effective dispersal of these agents is not a trivial matter. In large water supplies, such attacks are virtually impossible; if the agents were dispersed efficiently as an aerosol, the help of a competent aerosol engineer and a meteorologist might be essential. Compared with nuclear explosives, despite the many difficulties associated with efficient dispersal, effective chemical, biological, and radiological attacks could readily be accomplished. Mass destruction, however reasonably measured, is technically feasible. But it is a myth that one can accomplish it by tossing a small quantity of some "supertoxin" into the water supply.

Bacteriological Warfare (BW) As A Terrorist Weapon

The terrorist literature has suggested that BW is a logical terrorist weapon, one against which defense is extremely difficult. The attacker may choose the agent, the time and the place, although there are constraints on all three. He may elect multiple-antibiotic resistant organisms or viruses (against which antibiotic therapy is largely ineffectual); vaccines are of little value against pulmonary plague or anthrax. Considering the lack of U.S. vaccine production and research capabilities, response might be significantly late.

A highly effective BW attack could be made using bacteria (plague or anthrax) in an aerosol cloud. R&D efforts can make significant contributions in (1) detection and satellite surveillance of aerosol clouds and BW agent production; (2) environmental countermeasures to destroy infectious agents in an aerosol cloud; and (3) personnel defense to kill infectious bacteria in the target organ (the lung), regardless of their antibiotic resistance.

1. Detection of infectious agent production and release. BW (and CW) production facilities are not basically identifiable by exterior features from commercial laboratory or production plant facilities. Overhead surveillance and intelligence collection must be targeted carefully to assure that research, production, storage, and distribution systems are detected and identified. On a more tactical level, local detection of aerosol clouds relies on inherent identifying characteristics. For example, protein toxins and some nerve gases, including Soman, are optically active; they interact differently with left and right circularly polarized light. The scatter of left and right circularly polarized laser light from such optically active compounds might serve for both intelligence gathering and to provide warning of attack. This method is potentially more sensitive than LIDAR (Light Detection and Ranging) methods. For laboratory tests, E. coli strain 1776 could provide "biological containment" (the organism would survive only in the laboratory). For subsequent field tests, further modifications of the organism by recombinant DNA methods may be necessary to render it totally incapable of survival in man.
2. Environmental countermeasures. A countercloud capable of destroying biological agents must be released at the instant an agent aerosol is detected. The tactical efficacy of such an approach is doubtful, but an effective method might involve drone aircraft directed to the cloud by computers coupled to the detection device described above. Ethylene oxide, lactic acid, O₃, systems generating short-lived free radicals (e.g., superoxide), lysozyme, and bacteriophage mixtures should be tested in the laboratory and later in the field to establish the most effective countercloud constituents.
3. Bacteriophage prophylaxis and treatment of bacterial infection. Bacteriophages specific for individual pathogens attack these bacterial cells and divert their metabolism to the production of more virus (bacteriophage). When up to a million bacteriophage are made the bacterial cells rupture releasing phage particles to destroy still more bacteria. Because of their specificity, the bacteriophage would not harm human cells. They could be administered individually with an atomizer (throat spray) to destroy the pathogens in the lung.

Chemical Warfare Agents

Urban areas, building, equipment and personnel are subject to contamination by chemical warfare agents. Rapid agent detection techniques must be developed for contamination avoidance as well as certification of hardware decontamination. The Air Force Scientific Advisory Board recently addressed these issues, looking at near-mid-, and long-term technological approaches, including laser-based methods for the detection of chemical warfare agents. Optical techniques appear to afford sensitive remote, point, and surface contamination detection capabilities.

Decontamination, discussed at length in a 1979 Army Science Board report, currently requires considerable logistics support, with large quantities of water, caustic or corrosive agents, and heavily protected crews. As noted in the 1981 Army Science Board Summer Study, "Equipping the Army, 1990-2000," genetic engineering appears to offer some hope of developing an enzymatic decontaminant safely usable on things and on people.

The Technological Challenges Ahead

Government's task — not just the military's — may be divided into four categories:

Prevention

The avoidance of terrorist incidents by denying access to suitable instruments (where possible) by successful protection of critical targets, or by deterring incidents through a combination of denial and protection.

Control

The timely establishment of command and control to assure an efficient response to an incident, with informational and decision-making provisions designed to seize the initiative from the terrorists.

Containment

Measures taken to delimit the terrorist act in a physical sense and to decouple it in a psychological sense from the intended political consequences. Actions to limit damage and provide emergency health care are included.

Restoration

Deliberate actions to conclude the incident and restore the situation to normal.

Prevention is a perceptual and policy issue as well as an intelligence matter, but physical security of sensitive installations is an important component. Little should be added to present R&D efforts—somewhat better sensors, stronger barriers, and more exotic booby traps. A lot of money has been invested in this area, possibly to the point of diminishing marginal returns. Yet, were intelligence measures and security measures to fail, government would be forced into the crisis management phase of the incident. The functions of control and containment provide the greatest policy, technology and management challenges.

Restoration, or the cleanup phase, is both a military and a civilian (FEMA) problem. The civil defense program within the United States is moribund. There is little or no federal leadership in this area. If some progress is to be made, the military will have to act.

The needs for counterterrorism technology are scenario-dependent. For example, airliner hijackings drove the development of metal detectors and micro-dose x-ray equipment now used in airports. The hostage seige (Munich, Entebbe, Mogadishu, Iran, and Princess Gate) justified para-military

rescue teams, which in turn inspired research for light weapons, forced entry means, incapacitating agents, specialized management information systems, and miniaturized encrypted communications. Since there are so many possible scenarios, the Army should develop a canonical set, simulate them from an operational perspective, and develop a counterterrorism technology program.

The biological and chemical threats indicate obvious priorities. Inexpensive techniques to defend civilian aircraft against heat-seeking rockets are prime candidates for further research. New technologies to deal with hostage-barricades (entry, surveillance, incapacitators, light, sound, microwaves, and electronic means for isolation) continue to be of utmost importance. Here, of course, "James Bond" gadgets are relevant; silent drills, clandestine TV systems, special dart guns, laser holography, immersing subjects in laser modulated sound, and the like.

From the opposite perspective, the "bag of tricks" must be stressed and categorized. (In fact, some scenarios may be derived by available technology.) The existent technologies should thus be reviewed from a functional point of view.

Sensors (detectors)—acoustic, optical, electromagnetic, chemical, biological.

Explosives - conventional, including shaped charges, concussion grenades, fragmentation weapons, etc.

Exotic devices - ultrasonics, laser beams, incoherent high intensity light, magnetically driven darts.

After initial screening or evaluation, such technologies can be matched with surveillance, area denial, and the more general requirements of containment and control.

A true systems analysis is needed, one which fully identifies costs and benefits if the Army is to broaden its future role in the area of counterterrorism. If senior Army leaders, in concert with appropriate Federal authorities, determine the need for such a mission, enabling legislation, program responsibility, and budget would be required.

Distribution

COPIES

Office Secretary of Defense

Secretary of Defense.....	1
Deputy Secretary of Defense.....	1
Under Secretary of Defense (Policy).....	1
Assistant Secretary of Defense..... (International Security Affairs)	1
Assistant Secretary of Defense..... (International Security Policy)	1
Under Secretary of Defense for Research and Engineering...	1
Assistant Secretary of Defense..... (Manpower, Reserve Affairs and Logistics)	1
Assistant Secretary of Defense (Public Affairs).....	1
Assistant Secretary of Defense (Health Affairs).....	1
Assistant Secretary of Defense (Legislative Affairs).....	1
General Counsel..... ATTN: Hon W. H. Taft IV	1
Director Program Analysis and Evaluation.....	1
Defense Science Board.....	1

Office, Joint Chiefs of Staff

Director, Joint Staff.....	5
----------------------------	---

Department of Defense

Defense Advanced Research Projects Agency.....	1
Defense Intelligence Agency.....	1
Defense Technical Information Center.....	12
Air Force Scientific Advisory Board.....	1
Naval Research Advisory Committee.....	1

COPIES

Office Secretary of the Army

Secretary of the Army.....	1
Under Secretary of the Army.....	1
Deputy Under Secretary of the Army (Operations Research)...	1
Assistant Secretary of the Army..... (Research, Development and Acquisition) Army Science Board	17

Army Staff

Chief of Staff.....	1
Vice Chief of Staff.....	1
Director of Army Staff.....	1
Comptroller of the Army.....	1
Deputy Chief of Staff for Logistics.....	1
DALO-SAZ.....	1
DALO-PLZ.....	1
DALO-AV.....	1
Deputy Chief of Staff for Operations and Plans.....	1
DAMO-ZD.....	1
DAMO-SS.....	5
DAMO-RQ.....	2
Deputy Chief of Staff for Personnel.....	1
Deputy Chief of Staff for Research, Development and..... Acquisition	1
Assistant Chief of Staff for Intelligence.....	5
Chief of Engineers.....	1
Chief of Army Reserve.....	1
The Surgeon General.....	1
National Guard Bureau.....	1

COPIES

MACOMs

US Army Forces Command.....	5
9th Infantry Division.....	1
US Army Training and Doctrine Command.....	5
US Army Materiel Development and Readiness Command.....	5
US Army Intelligence and Security Command.....	5

ASB Member

Dr. Robert H. Kupperman.....	1
------------------------------	---

DATE
ILME